НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №3, 2011

УДК 621.396.13:004.056.5

Антонов В.В., Конахович Г.Ф., Козлюк І.О.

ОСОБЛИВОСТІ ПЕРЕДАВАННЯ ЗАХИЩЕНОГО МОВНОГО ТРАФІКА ЧЕРЕЗ СТАНДАРТНИЙ РАДІОКАНАЛ АВІАЦІЙНИХ СИСТЕМ ЗВ'ЯЗКУ

В статті проаналізовано технології передавання мовного трафіка. Визначено особливості та швидкість передавання цифрового потоку. Розглянуті загальні принципи побудови та дії вокодерів, а також основні типи вокодерів. Запропоновано передавання захищеного мовного трафіка через стандартний радіоканал авіаційних систем зв'язку з застосуванням вокодерного утиснення мовного сигналу і наступним його криптографічним шифруванням.

Визначення проблеми та постановка завдань. Проблема полягає в тому, що існуючі технології передавання конфіденційної мовної інформації через стандартний вузько смуговий авіаційний радіоканал не здатні задовольнити в комплексі існуючі норми щодо критеріїв захисту інформації, розбірливості прийнятих мовних повідомлень та забезпечення стабільності зв'язку. Тому для визначення шляхів вирішення цієї проблеми доцільно виявити особливості передавання захищеного мовного трафіка через стандартний радіоканал авіаційних систем зв'язку.

Загальноприйнята класифікація технологій передавання захищеного мовного трафіка надана, зокрема, у [1,стор.3]. Згідно цієї класифікації розрізняють три основних класи технологій передавання закритого мовного сигналу, що розрізняються за способом передавання у каналах зв'язку: аналогове скремблювання мовного сигналу, дискретизація мовного сигналу з наступним його шифруванням та вокодерне утиснення й дискретизація мови з наступним її шифруванням. Аналогові скремблери не здатні забезпечити високий ступінь захисту мовних повідомлень, що є необхідним для критичних авіаційних застосувань, і тому у даній роботі не розглядаються. Методи дискретизації мовного сигналу з наступним його шифруванням мало придатні для передачі через стандартний радіоканал авіаційного зв'язку, якщо мати на увазі, що ширина спектру неутисненого мовного сигналу займає смугу приблизно 3,3кГц, а для досягнення високої якості сприймання мови необхідне співвідношення сигнал/шум має бути у діапазоні 25 – 30 дБ [2]. За цих умов, згідно Шеннону [3], має забезпечуватися швидкість передавання даних на рівні 33кбіт/с, не менше, що не є реальним для більшості авіаційних застосувань. Вокодерне утиснення й дискретизація мови з наступним її шифруванням не потребує широкої смуги частот каналу і може здійснюватися у цифрових вузько смугових системах зв'язку. Тому цей клас систем закриття мовного сигналу може знайти застосування в авіаційних телекомунікаціях.

Особливості передавання мовної інформації через вузько смуговий канал зв'язку. Існує велика кількість методів утворення захищеного каналу передачі мовної інформації [1], деякі із котрих забезпечують можливість її транспортування через вузькосмуговий канал. Проте для цього каналу має місце фундаментальна закономірність: для забезпечення більш високої якості відтворення мови на приймальній стороні необхідно забезпечити за інших рівних умов більш високу швидкість передачі даних через канал. Зокрема, дискретизація та передача звукового сигналу на швидкостях 30 – 60 кбіт/с дозволяє у повній мірі відновити будь-який звук – шуми, музику, голос. З іншого боку, якщо обмежитися вимогою розпізнавання лише смислового змісту отриманого мовного повідомлення (тобто, отримання певного еквіваленту друкованого тексту, що не несе індивідуальних ознак голосу та інтонацій), то необхідно забезпечити швидкість передавання не більше кількох сотень біт/с. Дослідження структури звуків людської мови показало, що для передавання не тільки тексту, але і індивідуальних особливостей голосу достатньо передавати цифровий потік на швидкостях 2 – 6 кбіт/с [1]. До особливостей передавання цього потоку слід віднести наступне.

1) Процес аналізу на передавальній стороні потребує проміжку часу не менше десятка мілісекунд (типовий інтервал аналізу 15–30 мс), тому на приймальній стороні мовний сигнал

відновлюється з певною затримкою, але ця затримка є суттєво меншою, ніж у скремблера, і для слухача є непомітною.

2) Оскільки алгоритм аналізу налаштований на максимальне використання особливостей усереднених характеристик голосу, то при виголошенні надзвичайно високих звуків та при певних звукосполученнях процес кодування може порушуватися та у відновленій на приймальній стороні мові виникають характерні «призвуки». Із тих же причин різноманітні шуми (зокрема, інші голоси) на передавальній стороні можуть суттєво негативно впливати на якість відновлення мови.

3) Кодуючий блок вокодера усі звуки, що виникають на передавальній стороні, представляє як компоненти мови однієї особи, що може призвести до помітних спотворень. Наприклад, якщо на мікрофон впливає механічний шум, то після кодування/декодування він може перетворитися на людський голос. Ця обставина накладає певні обмеження на використання вокодерної апаратури.

Слід зазначити, що при вокодерній обробці параметри мовного сигналу на малих інтервалах часу (до 30мс) можуть розглядатися як постійні [4]. Через суб'єктивний характер прийнятих методик оцінки якості передавання мови трудно визначити формальний зв'язок між інтервалами аналізу параметрів мовного сигналу та показниками якості синтезованих мовних повідомлень. Проте можливо однозначно стверджувати: чим коротше інтервал аналізу, тим точніше можна представити динаміку мови і, отже, отримати більш якісний синтезований сигнал. Але при цьому необхідно забезпечити більш високу швидкість передачі даних. Опубліковані дані свідчать [1], що у більшості випадків на практиці використовуються 20-мілісекундні інтервали аналізу, а в залежності від вимог до показників якості синтезу мовних повідомлень необхідна швидкість модемної передачі знаходиться у діапазоні 2400- 9600 біт/с. Зокрема, так звана комерційна якість синтезованої мови (коли рівень розбірливості мови за звичайних умов задовольняє більшість користувачів) забезпечується на швидкостях 2400 - 4800 біт/с [4]. Проте критичні авіаційні застосування потребують більш високої якості передавання мови і, отже, більш високих швидкостей передавання даних – 6200 біт/с і більше.

Способи передавання захищеного мовного трафіка через вузько смуговий канал. Для того, щоб відносно широкий спектр якісного мовного сигналу було можливим транспортувати через вузьку смугу пропускання мовного тракту стандартного авіаційного радіоканалу, необхідно на передавальній стороні здійснити компандування цього сигналу (тобто, утиснути ширину його спектру), а на приймальній стороні здійснити його експандування (тобто, цей спектр відновити). Можливі два способи компандування мови - безпосередній та параметричний. Принцип безпосереднього компандування через технічні труднощі на практиці не знайшов застосування, в той час як параметричне компандування широко використовується у реальних системах зв'язку.

Під час компандування знижується інформаційна надмірність людської мови. Це зниження досягається параметризацією мовного сигналу, при якій зберігаються істотні для сприйняття характеристики мови. Вокодер, аналізуючи форму мовного сигналу, робить оцінку параметрів змінних компонентів певним чином обраної моделі генерації мови й передає ці параметри у цифровій формі через канал зв'язку на синтезатор, де відповідно до цієї моделі по прийнятим параметрам синтезується мовне повідомлення. Оскільки обрана модель генерації мови завжди передбачає повільну зміну її параметрів в процесі здійснення сеансу зв'язку, то для передачі цих параметрів на приймальну сторону широка смуга каналу не є потрібною. Залежно від прийнятої системи параметрів, завдяки яким виконується відновлення первісного мовного сигналу, розрізнюють основні типи вокодерів: смугові, формантні, гармонічні та фонемні.

Розглянемо загальний принцип дії вокодера, який пояснюється узагальненою блок-схемою (рис.1). Головними частинами вокодерного тракту є: аналізатор, який виявляє параметри мовного сигналу; система передавання, яка забезпечує проходження інформації про ці параметри через канал зв'язку у вузькій смузі частот; синтезатор, який відновлює

первісний мовний сигнал. Аналізатор вокодера складається із пристрою для виділення параметрів мовного сигналу A_1, .., A_i, ..., A_k та схеми виділення основного тону ОТ. Для того щоб на приймальному кінці мова могла бути відновлена з достатньо високою розбірливістю й хоча б із задовільною якістю звучання, потрібно передати в синтезатор наступні сигнали:

1) Сигнал про те, чи передається в певний момент часу звук з тональним (Т) або шумовим (Ш) збудженням; ця інформація передається параметром Т - Ш (тон-шум);

2) Якщо передається тональний звук, тоді має бути переданий сигнал про частоту основного тону ОТ – параметр F_0;

3) Сигнали, за якими можна відновити миттєвий спектр звуку і його зміни з часом, тобто параметри A_1, .., A_i, ..., A_k.

Параметри A_1, .., A_i, ..., A_k формує пристрій для виділення параметрів мови, конкретний принцип дії якого залежить від типу вокодера.

Сигнали F_0 і Т - Ш «витягуються» з мови схемою виділення ОТ, яка будується незалежно від конкретного типу вокодера. Варіант структури такої схеми показано на рис.2.

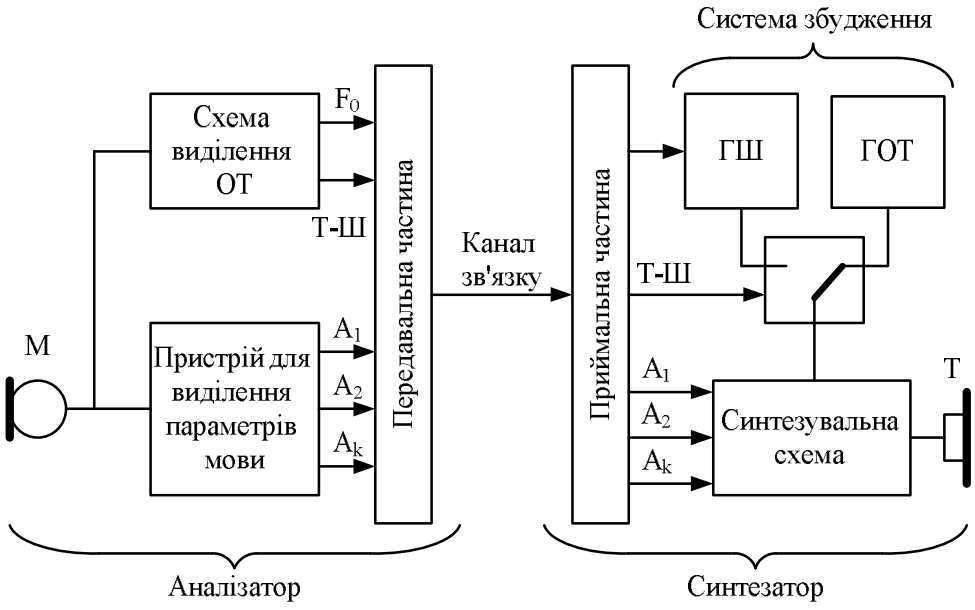

Рис. 1. Узагальнена блок-схема вокодера

Мовний сигнал, який надходить до входу системи, одночасно діє на два блоки – на визначник характеру збудження Т - Ш та на виділювач ОТ. Перший з них аналізує характер спектра і видає на вихід сигнал «Тон» або «Шум». Другий блок, який складається із смугового фільтру СФ, що виділяє діапазон частот, у яких може знаходитись ОТ, частотоміра та вихідного фільтру низьких частот ФНЧ, що визначає частоту ОТ і видає на вихід схеми сигнал F_0 у вигляді постійної напруги, величина якої пропорційна частоті ОТ f_0.

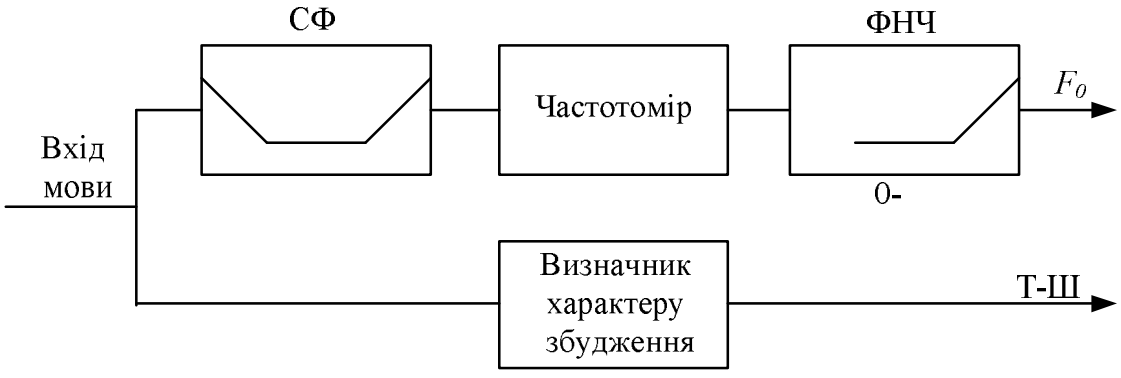

Рис. 2. Схема виділення ОТ

У синтезаторі вокодера також можна виділити дві основні частини, які функціонально зв'язані з відповідними двома частинами аналізатора. Це – місцеві джерела збудження у складі генератора шуму суцільного спектру ГШ, генератора основного тону ГОТ та перемикача Т – Ш, а також синтезуючої схеми. Остання є не що інше, як модель мовного тракту змінної форми спектра, створеного збуджувачем (ГОТ або ГШ), відповідно до сигналів, які надходять від аналізатора.

Синтезатор отримує сигнали про параметри мовного процесу Т - Ш, F_0 , A_1, .., A_i, ..., A_k . Кожний з них діє на свій приймальний пристрій. Якщо у певний момент часу передається глухий звук, тоді сигналом Т-Ш перемикач Т-Ш установлюється в положення «Ш» і на синтезуючу схему подається рівномірний суцільний спектр від ГШ. Якщо вимовляється дзвінкий звук, то перемикач Т-Ш переводиться в положення «Т» і на синтезуючу схему буде видаватися дискретний спектр гармонік ОТ частоти f_0, значення якої беруть відповідно до значення рівня сигналу F_0 .

Одночасно сигнали $A_i, ..., A_k$ потрапляють на синтезуючу схему. Ці сигнали змінюють обвідну суцільного або дискретного спектра, формуючи тим самим спектральні максимуми та мінімуми відповідно до змінних спектра первісного звуку. Синтезований таким чином сигнал надходить на мовний вихід синтезатора.

Відношення ширини спектра вихідної мови (тобто, некомпресованої мови) F до ширини спектра компресованої мови F_K називають коефіцієнтом компресії вокодера:

$$\eta = F / \ F_k , \tag{1}$$

Коефіцієнт компресії вокодера будь-якого типу можна орієнтовно визначити, якщо є відомою кількість параметрів m, які передаються через канал зв'язку, і ширину смуги частот Δf , що потрібна для передавання кожного параметра.

Але для підвищення надійності передавання беруть смугу частот шириною $2\Delta f$. Тоді ширина смуги частот компресованого сигналу визначається як

$$\mathrm{F_K} = 2m * \Delta f , \tag{2}$$

Розглянуті загальні принципи будови та дії вокодерів притаманні вокодерам різних систем. По суті, вокодери відрізняються між собою лише принципом дії пристрою для виділення параметрів мови в аналізаторі та синтезуючої схеми у синтезаторі. До найбільш розповсюджених типів вокодерів належать смугові вокодери та вокодери із лінійним провісником (ліпредери). Смуговий вокодер передає амплітуди кількох частотних смуг мовного спектру. Кожний смуговий фільтр такого вокодеру збуджується при появі енергії мовного сигналу у його смузі пропускання. Оскільки спектр мовного сигналу змінюється відносно повільно, то набір амплітуд вихідних сигналів фільтрів утворює придатну для вокодерного зв’язку основу. У синтезаторі на приймальній стороні параметри амплітуди кожного каналу управляють коефіцієнтами підсилення відповідного фільтру, характеристики котрого є подібними характеристикам фільтру аналізатора. Таким чином, структура смугового фільтра базується на двох блоках фільтрів – для аналізу мови на передавальній стороні і для її синтезу на приймальній стороні системи зв’язку. Збільшення кількості частотних каналів покращує розбірливість мови, але при цьому передача через канал має здійснюватися з більшою швидкістю.

Практичними дослідженнями встановлено, що для визначення смислового змісту мови достатньо утворити у складі смугового вокодеру 16 – 20 частотних каналів та забезпечити швидкість передачі даних 2400 біт/с. Але цього, на жаль, недостатньо для якісного передавання мови, у т.ч. і через авіаційний радіоканал.

Системи цифрового закриття мови на базі смугових вокодерів детально розглянуті у [4]. Зазвичай смугові фільтри у цифровому виконанні будуються на базі аналогових фільтрів Баттерворта, Чебишева, еліптичних та ін. Кожен 20-мілісекундний проміжок часу кодується 48 бітами, із них 6 біт відводять на інформацію про основний тон, один біт – на інформацію про «тон-шум», 41 біт відображає значення амплітуд сигналів на виході смугових фільтрів.

Найбільше розповсюдження серед систем цифрового кодування мови з наступним шифруванням отримали вокодери з лінійним провісником (ЛПР). Математичне відображення моделі цифрового фільтру, що використовується у вокодері ЛПР, має вигляд шматково-лінійної апроксимації процесу формування мови із певними спрощеннями, а саме: кожен поточний відлік мовного сигналу є лінійною функцією P попередніх відліків. Незважаючи на недосконалість такої моделі, її параметри забезпечують прийнятне відтворення мовного сигналу. У вокодері ЛПР аналізатор здійснює мінімізацію помилки прогнозу, що являє собою різницю між поточним відліком мовного сигналу та середньо ваговою сумою P попередніх відліків, де P – порядок прогнозування, а вагові коефіцієнти є коефіцієнтами лінійного прогнозування. Оцінка якості здійснюється за мінімумом середньоквадратичної величини помилки прогнозування. Існує кілька методів мінімізації помилки. Але загальним моментом є те, що при оптимальній величині коефіцієнтів прогнозування спектр сигналу помилки наближається до білого шуму, а сусідні значення помилки мають мінімальну кореляцію.

У вокодері із лінійним провісником мовна інформація передається трьома параметрами: амплітудою, рішенням «сигнал-тон» та періодом основного тону для вокалізованих звуків. Окрім того, передаються через канал коефіцієнти прогнозування. Зокрема, згідно федерального стандарту США, період аналізованого проміжку мовного сигналу складає 22,5 мс, що відповідає 180 відлікам при частоті дискретизації 8 кГц. Кодування у цьому випадку здійснюється 54 бітами, що відповідає швидкості 2400 біт/с. При цьому 41 біт відводиться на кодування десяти коефіцієнтів прогнозування, 5 – на кодування величини амплітуди, 7 – на передачу періоду основного тону, та 1 біт визначає рішення «тон-шум». Подібне кодування передбачає, що усі параметри є незалежними, проте у натуральній мові параметри є корельованими. Це означає можливість суттєвого зниження швидкості передачі без втрати якості, якщо правило кодування оптимізувати з урахуванням залежності усіх параметрів. Такий підхід відомий під назвою векторне кодування. Його застосування до вокодеру ЛПР дозволяє зменшити швидкість передачі даних до 800 біт/с із незначною втратою якості відновленої мови. Проте усі вищезазначені параметри вокодерного зв'язку не придатні для критичних авіаційних застосувань, оскільки вони не забезпечують прийнятний рівень якості розбірливості мови на приймальній стороні каналу.

Щодо особливостей передавання захищеного мовного трафіка через стандартний радіоканал авіаційних систем зв'язку, то слід зазначити наступне.

1) Стандартний радіоканал авіаційного зв'язку є вузько смуговим. Тому в якості технології, найбільш придатної для забезпечення вимог критичних авіаційних застосувань, слід розглядати вокодерне утиснення мовного сигналу з наступним його шифруванням засобами, що реалізують один із ефективних алгоритмів криптографічного шифрування. У цьому випадку існує можливість реалізації технологій передавання захищеного мовного трафіка як з високими рівнями захисту, так і з високими рівнями якості прийнятих мовних повідомлень.

2) Високий рівень якості прийнятих мовних повідомлень досягається лише за умови забезпечення відносно високої швидкості передачі вокалізованих сигналів (якщо мати на увазі вузьку смугу пропускання каналу) у діапазоні 6200 – 9600 біт/с. На теперішній час цей діапазон швидкостей здатні забезпечити лише когерентні системи модемного зв'язку. Проте когерентним системам притаманний певний рівень нестабільності зв'язку, що пов'язаний із роботою систем фазової синхронізації. Внаслідок впливу різного роду завад спостерігаються відносно часті зриви фазової синхронізації з наступними відносно тривалими періодами відновлення синхронізації, що є негативним фактором, який обмежує використання сучасних

систем захисту мовної інформації в режимі інтенсивного мовного діалогу через вузькосмуговий канал. Тому актуальним є завдання розробки некогерентних систем, які були б здатними забезпечити вищевказаний діапазон швидкостей передачі, не порушуючи при цьому норм щодо завадостійкості та енергетичного бюджету стандартного радіоканалу авіаційного зв'язку.

Висновок. Із всієї множини існуючих технологій необхідні показники ефективності захисту та якості передавання мовних повідомлень у критичних авіаційних застосуваннях здатні забезпечити лише низькошвидкісні вокодерні системи зв'язку у комбінації із стійкими криптографічними засобами.

ЛІТЕРАТУРА

1. Дворянкин С.В., Девочкин Д.В. Методы закрытия речевых сигналов в телефонных каналах //Защита информации.- СПб.: Конфидент, №5, 1995, с. 45 – 54.

2. Петраков А.В., Лагутин В.С. Защита абонентского телетрафика. - М.: Радио и связь, 2001, 504 с.

3. Антонов В.М., Пермяков О.Ю. Комп'ютерні мережі військового призначення. - К.: "МК-Прес", 2005. - 320 с.

4. Єремеєва А.В. Оцінка якості відновлення мови при використанні смугового вокодера в захищених каналах // Дипломна робота випускника освітньо-кваліфікаційного рівня «Магістр». –К.: НАУ, 2009.

Надійшла: 29.09.2011

Рецензент: д.т.н., проф. Юдін О.К.